Industry Working Paper Series 07-01

KYC for Shell Companies

Rohan Bedi*
NUS Business School
National University of Singapore

*Executive-in-Residence
Saw Centre for Financial Studies
NUS Business School
National University of Singapore
Singapore 117592
Tel: 97629060
Email: rohanbedi@rohanbedi.com
http://www.rohanbedi.com
KYC for Shell Companies

Abstract
This paper provides an in-depth study on Know Your Customer issues associated with Shell companies or paper companies i.e., companies that engage in no apparent business activity and that only serve as a conduit for funds or securities. It highlights that shell companies can be incorporated in any jurisdiction but those setup in offshore financial centers (OFCs) are preferred by money launderers and terrorist financiers. This is because of the lower standards of corporate transparency combined with high levels of banking secrecy. Bearer share companies and trust structures further help to reduce transparency. Shell companies are a deadly tool used for decades to move the proceeds of crime under the guise of legitimate business transactions. Cross-border cash smuggling and placement using shell companies is now the flavour of the season for terrorist financing. Regulation of company and trust formation agents for AML is a must to ensure better due diligence and transparency.

February 2007

Keywords: Shell Companies, KYC, AML, CFT, Know Your Customer, Money Laundering, Financial Crime, Risk Management, Fraud
## Contents

<table>
<thead>
<tr>
<th>No.</th>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Country Risk</td>
<td>4</td>
</tr>
<tr>
<td>2.</td>
<td>Key KYC processes</td>
<td>12</td>
</tr>
<tr>
<td>2.1</td>
<td>Ownership Basics</td>
<td>13</td>
</tr>
<tr>
<td>2.2</td>
<td>Age and Name</td>
<td>19</td>
</tr>
<tr>
<td>2.3</td>
<td>Documentation</td>
<td>21</td>
</tr>
<tr>
<td>2.4</td>
<td>PICs in Trust Structures</td>
<td>27</td>
</tr>
<tr>
<td>2.5</td>
<td>Verification – High-Risk Databases</td>
<td>29</td>
</tr>
<tr>
<td>2.6</td>
<td>Know Your Employee Controls</td>
<td>31</td>
</tr>
<tr>
<td>2.7</td>
<td>Ongoing Transactions Monitoring</td>
<td>32</td>
</tr>
<tr>
<td>3.</td>
<td>Conclusion</td>
<td>36</td>
</tr>
</tbody>
</table>
1. Country Risk

Shell companies are commonly understood as companies that exist only on paper but have substantially no operations or assets\(^1\). They may well purport to have employees, a local office, a telephone number and even a website, but a close review would reveal that these are just “purchased” branding services. They are pivotal in money laundering and some terrorist financing schemes, in the placement stage (e.g., in fraud schemes; in terrorist financing schemes which involve placement of cash smuggled); in the layering stage to pass money through (parties in international wire transfers) to confuse the trail by moving monies between multiple jurisdictions, companies and bank accounts; and in the integration stage to, for example, invest in real estate, in loan-back arrangements, to facilitate investments in self-owned hedge funds, generate bogus capital gains on options trading, and as employee income.

Shell companies are used not only to launder money, but also to generate it, e.g. from earnings of a criminal offence (money with illegal origin) or as windfalls (earnings) of tax evasion (money with legal origin)\(^2\). They have been used in pump and dump, credit card bust out, fraud (including mortgage fraud, securities fraud, employee asset misappropriation fraud\(^3\)), over invoicing and false invoicing schemes. Offshore shell companies have been used to trade in derivatives that replicate insider trading opportunities and more directly for insider trading. They have played a role in facilitating the illicit trade in conflict diamonds (“blood diamonds”). Shell banks have been abused by launderer and terrorist alike to act as a front to deposit and move cash

---

\(^1\) US SEC states that shell companies have “no or nominal operations and either no or nominal assets or assets consisting of any amount of cash and cash equivalents and nominal other assets”


\(^3\) AICPA [http://www.aicpa.org/PUBS/jofa/jul2002/wells.htm](http://www.aicpa.org/PUBS/jofa/jul2002/wells.htm)
and monetary instruments especially via wire transfers. Shell companies exploit correspondent banking relationships (including with shell banks) to transfer funds. Identifying shell companies via wire transfer records is extremely difficult.

Nonetheless, most shell companies are used for legitimate purposes in tax planning structures, to facilitate domestic and cross-border currency and asset transfers and corporate mergers, and as Personal Investment Companies (PICs) used for holding assets (e.g. stock, property, intangible assets (IPR)) including with trust structures as in private banking. Private banking is a high-risk industry and their role includes facilitating the setting up of their clients shell companies (PICs) and related nominee arrangements.

Shell companies are also used legitimately in shipping (to establish a link with the flag state i.e., to effect a change in corporate domicile) but this practice has been abused by terrorists seeking anonymity, to move goods and also to earn legitimate monies to fund terrorism. Similarly, shell companies have been exploited by air cargo companies that specialize in transporting arms to conflict zones.

The most exploited by criminals are non-listed shell companies that may even be registered as service providers or manufacturers. In addition to semi-legitimate front businesses, drug traffickers use these shell companies (often under the guise of being a cash-intensive business) to deposit cash and to wire transfer funds between accounts often using *fake invoices*. Moreover, listed companies that have become defunct and continue to maintain their public trading status, also become shell companies. These companies generally have no business operations, little if any assets and trade for pennies. Private companies that want to become public can purchase control of these listed shell companies, and then potentially misuse their new status for fraud and abuse in the securities market (e.g. “pump and dump” schemes).
Shell companies can in theory be incorporated in any jurisdiction. However, for reasons of lack of transparency (thanks to minimal information required to be submitted and banking secrecy laws), the shells used in criminal schemes are most often setup in offshore centers.

Offshore centers typically have zero/low taxes, fast company incorporation, offer USD accounts, do not put any restrictions on transfer of funds or profits, may also offer bearer share companies and trust structures that facilitate a lack of transparency. Their AML laws are either not stringent or not enforced. Specifically, their company and trust formation agents may not be required to be registered (with “fit and proper” requirements) and may not be regulated for AML. Hence requirements for checking for beneficial ownership at company/trust formation may not be inscribed into law.

The shell companies are often incorporated under the International Business Companies (IBC) act of the offshore financial center (OFC) which typically allows them to conduct their business solely with non-residents and they do not have any physical presence in the country. Reporting requirements are also relatively low. Nonetheless, not all offshore centers have an IBC act and they differ on the degree of due diligence at company incorporation and corporate transparency/banking secrecy offered. Many have signed agreements that require them to share information with countries like the US for criminal investigations. Offshore centers are important to the world economy given that somewhere between US$7 and US$10 trillion worth of funds is held with them.
Offshore Financial Centers (OFCs)\textsuperscript{4}

These jurisdictions are often sovereign states but not necessarily so. They may be a free zone within a city, such as Dublin, Ireland. They may also be political subdivisions within a sovereign state, such as Madeira or Hong Kong. Many resist the categorization as offshore.\textsuperscript{5}

The Caribbean
Anguilla, Antigua and Barbuda, Aruba, Bahamas (Nassau), Barbados, Belize, Bermuda, the British Virgin Islands (BVI), Cayman Islands\textsuperscript{6}, Costa Rica, Dominica, Grenada, Guatemala, Montserrat, Netherlands Antilles, Panama, Saint Kitts and Nevis, Saint Lucia, St. Vincent and the Grenadines; the Turks and Caicos Islands; and Uruguay.

Europe
Andorra, Austria, Campione, Cyprus, Czech Republic, Gibraltar, Guernsey/Sark/Aldernay, Ireland (Dublin), Isle of Man, Jersey, Latvia, Liechtenstein, Luxembourg, Madeira, Malta, Monaco, Montenegro, Switzerland, and the Turkish Republic of Northern Cyprus.

Asia and the Pacific
Bangkok International Banking Facilities (BIBFs), Brunei, Cook Islands, Hong Kong Special Administrative Region, Malaysia’s Labaun Island, Macau, Marianas, Marshall Islands, Nauru, Niue, Western Samoa, Singapore, and Vanuatu.

Middle East
Bahrain, Dubai and Lebanon.

Africa
Liberia, Mauritius, Seychelles, and Tunisia.

\textsuperscript{4} A US 2007 bill ‘Stop Tax Haven Abuse Act’ lists a number of these as “Offshore Secrecy Jurisdictions”.

\textsuperscript{5} The Changing Shape of Offshore Jurisdictions, Colin Powell, 5 Sept 2002.

\textsuperscript{6} Cayman Islands is the 5\textsuperscript{th} largest center for bank deposits worldwide.
Of the above centers, some have ‘equivalent’ status with the US, UK by virtue of being FATF members/ well regulated, e.g. Singapore and Hong Kong. Singapore is now the third largest center for Private Banking - it has a low domestic crime rate and its AML regulations are generally well respected. Hong Kong is regarded as higher-risk because of the domestic crime situation and its role in money transfers from China.

Hong Kong is highlighted as high-risk by the Dept of State (INCSR) annual report. It states that many of the more than 500,000 IBCs created in Hong Kong are owned by other IBCs registered in the British Virgin Islands and many of the IBCs are established with nominee directors. They state that “the concealment of the ownership of accounts and assets is ideal for the laundering of funds.” Furthermore, Hong Kong-registered companies figure prominently in schemes to transfer corruption proceeds and in tax evasion recycling schemes in the People’s Republic of China.

Some jurisdictions such as the Cayman Islands, Bahamas, Jersey, and Isle of Man do comply with the FATF recommendation to identify the owners of the companies they establish. It can be argued that all are not equally competent at this.

Nonetheless, it is becoming increasingly commonplace to find an offshore connection to security frauds and other major sophisticated white-collar crimes.

**UK & US - Vulnerable**

At its simplest, the term "Offshore" refers to the provision of financial services to non-residents. Using this definition, London, New York and Tokyo are in a similar space and the IMF calls them International Financial Centers. The biggest center is London albeit the standards of due
diligence in bank account opening are high and banking secrecy laws are no serious impediment to criminal investigations.

However, contrary to popular perception, it is not just offshore companies and trusts that are susceptible to abuse by criminals. In the UK, the Performance and Innovation Unit Report, “Recovering the Proceeds of Crime,” noted that UK shell companies were seen as often involved in complex money laundering operations, with criminals benefiting both from the ease of incorporation in the UK, and from the maintenance of secrecy of beneficial ownership of UK companies. This underscores the importance of also regulating company and trust service providers for AML.7

The FBI believes that US shell companies and bank accounts are being used to launder as much as US$36 billion a year from the former Soviet Union8. Specifically, in the US, the states of Nevada, Wyoming and Delaware have been exploited in many criminal schemes as they facilitate ease of setup and lack of transparency similar to many other offshore centers9.

The three US states have four common characteristics: shareholders' identities do not have to be revealed to the authorities; company meetings can be held anywhere in the world; no minimum capital requirements; and one-person companies are allowed (although this is also the case in the UK). The typical company formation agent delivers the incorporation documents directly to the state agency, albeit intermediaries such as attorneys or accounting firms are typically involved. The agent has no knowledge of the identity of the beneficial owners, and takes the officer and director information at face value, without any enquiry or due diligence.

---

7 Transparency International’s report “Corruption and Money Laundering in the UK: One Problem, Two Standards”, October 2004
8 GAO Report “Company Formations: Minimal Ownership Information is Collected and Available”, April 2006
Nevada and Wyoming also permit bearer share companies. A US company address lends credibility in global trade and access to US bank accounts.

The US was formally criticized in the Financial Action Task Force (FATF) 2006 review of its Anti-Money Laundering (AML) laws and now has two years in which to comply, or risk expulsion from the FATF.

**US SAR Review**

The US FinCEN identified 1,002 Suspicious Activity Reports (SARs) (also called suspicious transaction report i.e., STR) filed from 1996 through the beginning of 2005 that reference activity that appears to be related to shell companies. These SARs reveal a wide variety of domestic and offshore financial center activity.

- Suspected *shell company* locations range from the US to the Cook Islands, Vanuatu, Bahamas, the UK, Panama, the Cayman Islands, Nigeria, and Antigua. SARs identify suspected *shell banks* in foreign locations such as Uruguay, the Cook Islands, St. Lucia, and St. Vincent/Grenadines.

- Many of the US-based suspected shell companies were observed to maintain banking relationships with Eastern European financial institutions, particularly in Russia and Latvia.

- US shell companies were used to perpetuate tax fraud in Russia, Latvia, Lithuania, and the Ukraine.

Besides the offshore havens, many other countries in Eastern Europe are being misused by launderers to setup and use shell companies and banks in money laundering schemes. According to the FinCEN 7th SAR Review, 2004:
The Eastern European Countries that were identified in US SAR narratives with *shell companies* included Armenia, Belarus, Bulgaria, Croatia, Cyprus, Czech Republic, Estonia, Georgia, Greece, Kazakhstan, Latvia, Lithuania, Moldova, Poland, Romania, Russia, Slovenia, Turkey, Turkmenistan, Ukraine, Uzbekistan and Yugoslavia.

The Eastern European Countries that were identified in SAR narratives with *shell banks* included Bulgaria, Cyprus, Estonia, Georgia, Kazakhstan, Latvia, Lithuania, Poland, Russia, Turkey, Ukraine and Yugoslavia.
2. Key KYC processes

The key Know Your Customer (KYC) processes will be viewed in the context of a bank account opening. Providing services to shell companies involves varying degrees of risk, depending on the ownership structure, nature of the customer, the services provided, purpose of the account, the location of services, and other associated factors. Business entities created in-house would be lower risk than those created externally.

The bank’s risk assessment of a business entity customer becomes more important in complex corporate formations. For example, a foreign IBC may establish a layered series of business entities, with each entity naming its parent as its beneficiary. Layers of ownership are devised to make it highly unlikely for relationships among various individuals and companies to be discerned, even if one or more of the owners is actually known or discovered.

The rule is that if the ownership structure is unduly complex and a bank is not satisfied that they know who the beneficial owners are, they should refuse account opening and file a SAR.

---

10 Because of the complexities in company account opening, many banks prefer separate account opening sections independent of the sales personnel.
12 US FFIEC Examination Manual '06, Business Entities (Domestic and Foreign) – Overview
2.1 Ownership Basics

It is important to understand the beneficial ownership of a company. The FATF defines beneficial owner as the natural person “who ultimately owns or controls a customer and/or the person on whose behalf a transaction is being conducted. It also incorporates those persons who exercise ultimate effective control over a legal person or arrangement.”

Control refers to the ability to influence directly the actions of a company or to make policy for the company. Usually, control is exercised by members of senior management (including directors especially for private limited companies) and can also be a function of the level of ownership in a company. In layered ownership structures it involves “looking through” the immediate levels of corporate ownership to the ultimate natural persons whose beneficial ownership exceeds a level that confers control. Control can also be established through the loans route without any equity being involved (a typology followed by the IRA).

Laundering schemes often involve multi-jurisdictional and/or complex structure of corporate entities and/or trusts. Tax, financial and legal advisors are generally involved in developing and establishing the structure which includes the use of nominee services.

Cases & Lessons

1. **PEP’s**: Ferdinand Marcos, the former President of the Philippines, looted his country by using offshore shell companies and offshore trusts. He bought an offshore company in the Isle of Man which then opened a bank account in the Caymans which was managed by a trust company in Bermuda. The Philippine National Oil Co. then made payments to this dirty money account. *Lesson: a money laundering scheme typically use more than one*

---

jurisdiction to create hurdles for investigators and a structure such as this should be a red flag.

2. **Nominees:** In 1996, the US regulators concluded a case in which “a private debt trader in New York, formerly a vice president of a major US bank, set up shell companies in Antigua with the help of one of the “big five” accounting firms. Employees of the accounting firm served as nominee managers and directors. The payments arranged by the accounting firm on behalf of the crooked debt trader included bribes paid to a New York banker in the name of a British Virgin Islands company, into a Swiss bank account; bribes to two bankers in Florida in the name of another British Virgin Islands corporation and bribes to a banker in Amsterdam into a numbered Swiss account”15. *Lesson: don’t let lawyer and accountant nominee names lull one into a false sense of security.*

3. **Fraud:** In a US "boiler room" or "bucket shop" scam, A.R. Baron & Co. pushed questionable stocks and specialized in market manipulation, unauthorized trading in customer’s accounts and countless other methods of taking advantage of innocent investors. They used Liberian shell companies and accounts in the Isle of Jersey to trade in the stock the firm was underwriting, a violation of US securities laws. They also sheltered their illegal profits - from tax authorities, creditors and the Bankruptcy Court - in a Cook Islands trust, which had a creditor unfriendly trust law. *Lesson: trust structures are a popular way of keeping the proceeds of fraud from being returned because of the costs and effort involved in recovery.*

The internet can help to find out more about the customers' business, establish whether nominee arrangements are in place, understand if the activity of a particular customer is unusual, and to find out both more negative and positive information on a client. Care should be taken to refer to reliable sources for which a list of websites needs to be built up for reference. A word of caution is that if the investigator is already using a good KYC

---

check product (that culls out risk related information including from internet and other sources) then he/she should be careful to avoid duplication.

For example, in a layered ownership structure, it is important for the bank to go backwards until the key shareholders (e.g. 5% or more) can be listed.

- If the ultimate shareholders, officers, directors, or authorized signatories turn out to be persons who are potentially nominees (company and trust formation agents, accountants, lawyers) then further investigation is needed to identify those they represent. Also, these nominees may not be regulated for AML causing additional risks.

- Where there are company directors and/or company shareholders, they need to be reviewed to understand who the ultimate beneficial owners are.

- If the directors and authorized signatories are different (typically the same for small private limited companies), this needs to be investigated and enhanced due diligence conducted on the authorized signatory, if warranted.

- If the authorized signatory is not an employee or director or shareholder, this is a red flag as often launderers only take on authorized signatory roles on their shell companies bank accounts (to keep their names off the company records).

- Google searches (and searches on the banks own database of customers and account parties (directors, share-holders, authorized signatories) to review for links to other companies) on the potential nominee names (individuals or entities) may help to confirm their status as a service provider. To a reasonable extent, name variations should also be considered during searches.

- A further check on their websites can also confirm if they are in the business of retailing “shelf companies”.
Find out how long the company is at its current address and verify this fact (where possible/considered necessary through onsite business premises visit using the banks arrangements in this regard, for example, with a firm of lawyers in Belize). Google search the company address to see if there are others using it that could indicate a mail-box/virtual office address. If the address is a virtual office address the chances are high that the same service provider is also providing the phone number listed on the application form. Depending on the package\textsuperscript{16} subscribed to, the telephone number can also be unique i.e., used only by the firm/local telephone listing/registered in its name (the virtual office would be listed under “vendor”) and may also be supported by a staff who picks up the phone and answers smartly in the name of the firm! Hence, check if the “vendors” name is also recorded and also when it was registered. Internet yellow pages are one source of information. Nonetheless, the overwhelming majority of ‘paper’ entities do not have a telephone directory listing and this is a red flag in itself. Moreover, if for example, the company was incorporated seven years ago and the address and telephone check only covers the last one year, further due diligence is necessary.

Enron, which was headquartered in the US, incorporated more than 600 subsidiaries in the Cayman Islands. Not a single listing was there for these companies in the local telephone directory nor any local office. These companies were used by Enron to hide massive losses as part of an elaborate fraud. Parmalat also exploited the Cayman Islands highlighting corporate governance issues. \textit{Nominee directors in offshore shell companies can be holding such positions in 100’s of such paper companies and play little or no role from a corporate governance perspective.} [In terms of controls on nominee directors, some jurisdictions do not recognize the concept of a nominee director i.e., a nominee director has to accept all the requirements and

\textsuperscript{16} The package may also throw in a state business license, an office that is staffed during business hours and 24 hours personalized voicemail.
obligations of a director. Others do not allow directors to be indemnified by the beneficial owner and others limit the number of directorships a person may hold.]

Understanding the nature and purpose of the intended business relationship is important. It is also important to understand the nature of the business and how long it’s been around (a review of the clients website (if any) should help with the basic information (albeit needing further verification), the source of funds of monies coming into the account, and the source of wealth (for large value relationships) of the owner or beneficial owner. Collecting some basic information on volume and value of expected transactions and validating this “expected” profile with the information on the company’s financials is necessary. This validation in theory depends on the audited balance sheet which may not be available as it may not be required if the underlying company is an IBC. Business registration searches, business license searches, industry & people directories, property searches, credit reports\(^\text{17}\) (where available e.g. Dun and Bradstreet, Standard and Poor’s), are all potentially useful sources of supporting information. If the customer is expected to maintain a deposit /assets under management of USD 1mio and above (i.e., Private Banking thresholds), the focus should be on estimating “liquid net worth” of the client. Liquid net worth is a measure of worth that only includes assets that can readily be turned into cash (for example in one week) without a major loss in value. This is typically recorded through first questioning the customer - this is then validated independently where possible. In general, where information is scanty and the monies/ risks involved are significant, suitable arrangements should be considered including third party reports\(^\text{18}\).

\(^{17}\) Ongoing monitoring for specific events (e.g. winding up petitions, court judgements, insolvency filings, dissolution filings, severe audit qualifications, change of company name) affecting credit risk, is possible in some centers like the UK. This should be considered in specific high-risk situations, where possible.

\(^{18}\) Firms in this space include Kroll, Control Risks.
Remember that there is a thin line between tax planning and tax evasion. A shell company set-up for tax planning purposes can well be a front for other nefarious activities. Hence tax planning should not be accepted easily as the reason for a particular paper company being setup. Typical tax evasion schemes use false invoices issued by offshore shell companies, to remit money out which then finds its way into offshore trusts. Best practice is that where there is reasonable cause to suspect, there a SAR is filed irrespective of whether the client claims tax planning as the underlying reason.
2.2 Age and Name

Shell companies are not always identified easily. Launderers are known to purchase shell companies that were incorporated earlier (“shelf companies”) e.g. 5 years ago (but have never been used) and pass them off as existing businesses. Prices for these companies vary depending on the age, where incorporated, whether identification numbers exist, whether it filed non-activity tax returns, previously had a bank account, or currently maintains a bank account. Basically, a launderer can develop a credit history more easily with a shelf company. Company formation agents can also sell some aged shelf companies that have established credit files, trade lines, bank accounts and even sales tax numbers!

Launderers may also purchase a very old company that was formerly a genuine business operation and that is no longer an active business – reactivating such a company to make it functional is a small expense. Occasionally, launderers also change the name and identity (objectives of the company) in order to for example, represent themselves as an 80 year old bank. The date in name tactic (e.g. ABC (1950) Ltd.) is also a common trick to inspire confidence. If the incorporation date is not actually 1950 then this is straightaway a red flag. Names that inspire confidence, e.g. “British Coca Cola Ltd.” may a complete sham. Hence for situations such as these, require the client to prove their long history of business operations.

All the above situations create additional due diligence requirements where reference to the online registry of companies in an offshore location may not divulge sufficient details. These registries differ in the information collected (mostly on legal ownership vis-à-vis beneficial ownership), updating of this information, and the public availability of this information. In most offshore centers the information available publicly is limited to the registration number, date of
incorporation and the name and address of the legal entities registered agent. However, in Bermuda, based on a small fee it is possible to review the companies file at the registrar of companies and its share register and list of officers and directors kept at its registered office.

In the UK, the registrar of companies offers more information: general company details, document images (documents filed since 1995), company reports, document packages, company directors' details, mortgage index, certified documents and certificates, dissolved companies, disqualified directors, and insolvency details. Hence changes in a companies name, objectives, directors and officers can be verified easily. It is also possible to use the “Monitor Service” to monitor for documents filings for the companies that one seeks to monitor.
2.3 Documentation

Whenever one is dealing with a company setup in an offshore jurisdiction, there are some key basic questions which set the tone.

- Is it a FATF member country or equivalent jurisdiction? Is it a former FATF black-list country (a favourite for laundering schemes)?
- Is the company listed or unlisted (higher-risk)? Are company and trust formation agents regulated or unregulated for AML? What about lawyers and accountants?

Based on the answers to the above, the comfort level with the inherent risks involved determines how much of documentation needs to be collected. Given below are the documentation options available. Not all banks will take the tough road of enhanced due diligence – many will simply turn down high-risk company account opening (e.g. BVI) if it was not set up by them through their arrangements (e.g. with third party firms or the banks subsidiary incorporation company). If a bank is not comfortable even after taking a high standard of documentation, it should consider declining account opening and filing a SAR.

Where the company is purported to be an old established concern, get the customer to prove his statements through Bank Statements, Bank References, etc. Find out for how long they had the earlier bank account, the kind of transactions put through the account and if they had an account executive servicing them (for further reference if required). Bank statements are a prime source of information and they should be reviewed thoroughly including a review of the volume of business, the parties to business transactions, and the centers being transacted with. If the clients are respected names, Client Referrals can also help. Ask them to show the Stock
Certificates to see the date of issue. If the company is an old company and the date on the stock certificates is recent, it’s worth investigating. Launderers do purchase failed or inactive companies and use them in schemes after replacing all the officers and directors\textsuperscript{19}. They also purchase legitimate operating companies which they then misuse to launder money through, reflecting in a significant increase in business volumes – this should reflect in the bank statements.

Ask for the last three years audited Annual Reports and Tax Paid Receipts, where available/applicable. For IBCs there may be no requirements for an audited annual report to be submitted to the registrar of companies and neither are there any requirements for payments of tax of any kind. Where these documents are made available, they are to be viewed as part of the overall facts of the case. While information on the company management may not be required in the company formation stage, it may be required to be filed in the annual report (where these requirements exist). Moreover, the requirements may not extend to the standard of beneficial ownership and nominee arrangements can still help retain anonymity. In any case, launderers prefer not to file the first annual corporate report and instead prefer to use a shell company for a transaction, dissolve it after a few months and move on to use other shell companies.

Also ask for an apostillee (certificate issued by the Secretary of State or other Notary regulating agency that proves the authenticity of a Notary’s signature and seal) of the notarized incorporation documents for account opening. Required account opening documentation includes Certificate of Incorporation, Memorandum and Articles of Association (and all amending resolutions), Business Registration Certificate, Corporate Resolutions by the directors authorizing the opening of the account/the appointment of signatories. Particular attention should

\textsuperscript{19} Depending on jurisdiction, this may or may not be verifiable in the Registry of Companies
be paid to articles of association that allow for nominee shareholders, board members, and bearer shares.

Where for example, a BVI offshore company’s bank account is being opened in another jurisdiction (assume Hong Kong (HK)) and the company is also establishing a place of business in HK, there certified true copies of the Certificate of Registration of the Overseas Company issued by the Registrar of Companies in HK; the Business Registration Certificate issued by the Business Registration Office in HK; and the Registration of an Overseas Company in Hong Kong (i.e. Form F1 prescribed by the Registrar of Companies in HK) and all subsequent notifications/amendments filed (e.g. change of directors, address etc.), are also required for bank account opening.

Another document is the Certificate of Good Standing which is a certificate issued by a Companies Registry official as evidence that a corporation is in existence and active and has complied with tax requirements, or that is has filed annual reports or has not yet filed articles of dissolution. The certificate may indicate one or all of these items. A word of caution is that in many jurisdictions minimal information is required to get this certificate and while it has a “feel good” factor to it, it is just one document.

Other certification could be to require that the company's corporate attorney (and not the lawyer/agent setting up the company) issue a Beneficial Ownership Certificate to the effect that they have reviewed the books and records of the corporation, and they should name the beneficial owners i.e., the controlling directors and significant shareholders (e.g. 5% or more of total shares) and enclose their identification documents duly attested. The firm issuing the certificate should be a large well known firm which should be verified. A copy of the stock

---

20 US FFIEC Examination Manual ’06, Business Entities (Domestic and Foreign) – Overview
21 US Shell Companies Flourish, World-Check article, Ken Rijock, 5 June ’06
register which details all certificates issued and outstanding should also be attached and should be reviewed by compliance as should the corporate minute book (which may or may not be maintained properly). To the extent that there are nominee shareholders, or the changes in shareholders are not reflected, the usefulness of the stock register gets reduced. Another document that should be part of the review (and copy enclosed) is the Certificate of Incumbency (also called Register of Directors etc.), a document typically issued by the local registered agent in the country of incorporation, confirming the identity of the signing officers of the company (sometimes it also confirms the names of directors and shareholders as well as minute book contents). Money launderers rarely ever obtain a corporate minute book and stock register for their shell companies i.e., these ownership records do not exist and hence certification of beneficial ownership should be difficult to obtain from a reputable law firm. Where there are requirements that the resident agents know the location of the stock register, the launderer places their stock register and bearer shares in an offshore entity, to ensure their anonymity (if asked who owns a particular entity, the resident agent then says that all he/she knows is that it is owned by an entity in an offshore country).

A Sworn Affidavit (approved bank format) should be taken from the beneficial owners providing a declaration of beneficial ownership and undertaking to inform if this changes. A copy of the stock certificates (both sides) should also be attached and should also be sighted. The shareholders can also be asked to self-attest the copy22.

On a risk-based basis, an annual certificate of good standing and certification/ declaration of beneficial ownership (and sighting the stock certificates again where considered necessary), annual report (where available), should be obtained as considered necessary. Check if the beneficial ownership has changed. Also check if the nominee arrangements have changed and

---

22 A stock certificate can always be endorsed after completing the bank account opening procedures.
whether this represents a change in beneficial ownership. Where there are changes, the new nominees and beneficial owners need to be identified/verified. The account activity needs to be reviewed to see if changes in ownership have been followed by a sudden spurt in business volumes. A periodic review (periodicity based on risk) of the adequacy of customer information is also a requirement by the FATF and in most regulations. The risk models cover country, business, entity, product and transaction and these should help slot a client as high, medium or low risk which would then determine the periodicity of review.

**Bearer Shares** are issued by the corporation upon formation and actually deem ownership of the corporation to the holder of the share i.e., the person who has physical possession of the shares. Bearer share companies have been used by money launderers to conceal ownership in numerous complex money laundering schemes aided by the banking secrecy of the jurisdiction. They have also been used in terrorist financing schemes. Bearer shares, when issued by an IBC, and when further insulated by a simple conveyance known as the "mini-trust," through which control of the IBC has been passed to the beneficial owner, provide nearly impenetrable layers of anonymity for the ultimate beneficial owner of the assets. BVI bearer share companies have been historically exploited for laundering. After 2003, while the BVI brought in controls related to bearer share companies, the registered shareholders of BVI companies could still be entities from jurisdictions where unrestricted bearer shares still reign - e.g., Nevis and Panama. For example, the launderer may incorporate a Panama Private Interest foundation\(^{23}\) to hold the registered BVI bearer shares.

- Where bearer shares are involved for new clients or those without well-established relationships with the bank, the shares should be taken into custody by the bank or an independent third party.

---

\(^{23}\) See [http://www.panamalaw.org/panama_foundations.html](http://www.panamalaw.org/panama_foundations.html)
Where this is not possible and the customer is well-known and established, a beneficial ownership declaration can be taken both initially as well as annually. They should be required to notify the bank immediately when the shares are sold, assigned or transferred. Many banks insist on physical presence of all directors of a private limited company, during bank account opening. In the case of most offshore companies, there is no meaningful difference between “pte ltd” and “ltd” and the latter should not inspire more confidence as the reporting requirements may be identical\textsuperscript{24}.

\textsuperscript{24} This is not the case in jurisdictions like Singapore where “ltd” companies have more requirements.
2.4 PICs in Trust Structures

Trusts often constitute the final layer of anonymity for those seeking to conceal their identity. Trusts are vehicles intended to separate legal ownership and beneficial ownership. Traditionally, trusts have been treated like contractual agreements between private persons and subjected to less regulation and oversight and to fewer disclosure requirements, thus making them susceptible to abuse. In most jurisdictions, no disclosure of the identity of the beneficiary or the settlor is made to authorities and trusts have been abused for money laundering purposes, particularly in the layering and integration stages. Recent changes in the trust laws of some jurisdictions (Cook Islands, Nevis, and Niue) have aided money launderers in their use of trusts to conceal identity and to perpetrate fraud25.

Shell companies are commonly used in trust structures as Personal Investment Companies (PICs) to hold assets (the PICs shares are held by the trust) while giving the settlor (person giving up asset irrevocably to the trust administration company (also called grantor)) a degree of control on the assets often allowed by the trust law of the relevant jurisdiction.

- This can reflect in a role for the settlor/ his/her relative as a “controller” of the trust (control stretching from consultation to consent) or the settlor being the beneficiary or holding a directors position in the PIC with control on the bank account.

- Asset protection “flee clauses” can provide a layer of protection by directing that the assets of the trust and information about the trust to be moved to another jurisdiction and new

---

trustees to be appointed upon the occurrence of certain events, such as a service of process or change in legislation\textsuperscript{26}. This protects the settlor against enforcement action.

- The jurisdiction of the trust may have a creditor unfriendly trust law that helps keep the proceeds of fraud from being returned.
- Furthermore, the trust laws may not require the names of the settlor and the beneficiaries to be placed in the trust deed.
- The trust laws may allow trusts to be revocable and of unlimited duration. Revocable trusts are used to insulate the grantor and beneficial owner and can be designed to own and manage the business entity, presenting significant barriers to law enforcement\textsuperscript{27}.
- Layered offshore trust arrangements are another favorite in which the beneficiary of a trust structure is another trust structure.

Banks should insist on a copy of the trust deed which must be subject to legal scrutiny. Since trust structures are usually used by private banking type clients (e.g., USD 1mio in assets under management), due diligence on the settlor of the trust must be to private banking standards on source of funds, source of wealth etc. The underlying reason for the trust structure should be understood. The key trustees (making investment decisions/ payment instructions), the settlor and beneficiaries (or class of beneficiaries) must be identified/ verified. Critical in this scrutiny is the review of the credentials of/ the identification of the trust administration company/ its officers/ its jurisdiction (whether regulated for AML to quality or not) and larger banks have a pre-approved list for this purpose.

\textsuperscript{26} OECD report “Behind the Corporate Veil”, 2001
\textsuperscript{27} US FFIEC Examination Manual ’06, Business Entities (Domestic and Foreign) – Overview
2.5 Verification – High-Risk Databases

Given the ease with which a new shell company/offshore bank\textsuperscript{28} account can be set up, there is a serious risk of fraud associated with offshore shell companies and offshore bank accounts. Many jurisdictions accept copies of all identifying documents by PDF email/mail. The documents are not always required to be notarized and a certificate from a CA can suffice (in many countries obtaining notarized/certified copies of forged documents is easy and inexpensive). The verification done by the company formation agents in many offshore jurisdictions, on the company information submitted/the identities of company officials, is also poor or non-existent. Given these facts, it’s quite easy for a money launderer to setup the company and also the offshore bank account using stolen identities and to operate under these identities. Once they have an offshore debit/credit card in hand, using their dirty monies becomes even easier.

Identity theft is difficult to detect and only in few countries like the US are there specialist database searches available which are used in knowledge-based authentication solutions\textsuperscript{29}. In any case, if the purpose of the launderer is only to setup the bank account and use his monies (integration stage laundering), he/she is likely to use an identity that has not been used before in any criminal act. Checks on registry of births, electoral rolls and credit agencies may not be useful as they may simply prove the genuineness of the identity which is being used for the first time by the wrong person.

Basically, as long as there is no face-to-face interface, the launderer can meet the requirements of attestation and even of notarization with relative ease. Some products like

\textsuperscript{28} Offshore banks can enjoy an easier standard of regulation than onshore banks (this is not true for all jurisdictions). This translates to lower standards of due diligence in account opening.

\textsuperscript{29} Combating Identity Fraud: An Overview Of Complementary Approaches http://risk.lexisnexis.com/literature/Combating_Identity_Fraud.pdf
World-Check’s passport check can add value if critical information has been tampered and the passport is a machine readable passport. If the only replacement is to the photograph (or the signature) then without physical examination of the identification document, spotting this is difficult (unless the persons photograph/ signature can be verified from some source). Furthermore, fake utility bills (for address proof) can be generated easily off a colour printer.  

Other know-your-customer databases (e.g. World-Check, Factiva, Complinet, LexisNexis) help to highlight negative information in the media on persons and entities and also cover sanctions. This covers politically exposed persons and suspect terrorists, terrorist financiers, money launderers and other bad guys and also highlights links between them. Factiva news service (database search) is also helpful for detailed information. Besides these, banks must build additional databases to cover IPR Theft perpetrators (from sources such as the ICC-CCS UK, MPAA etc.), lost and stolen passports, internal databases that include their own SAR filing (with the fact of filing suppressed) etc. Other databases that can be accessed on a case-by-case basis include bankruptcy/winding-up search, civil litigation search and criminal conviction search (e.g. LexisNexis). The company and its officers, directors and shareholders should be reviewed against these databases as considered appropriate.  

The Wolfsberg Group of Banks believes that public authorities should make publicly available lists of shell banks remaining in operation. They are not convinced that it is otherwise possible to identify shell banks simply from their transactional activity via an institution, unless the shell bank is a customer of the institution, in which case the institution should in any event close the relationship.  

---

30 In the UK a single document e.g. passport can be used for both the identity proof and the address proof. This of course also reflects confidence in the UK passport issuance process.

31 Differences exist between existing vendors in terms of breath of coverage and information collection processes.
2.6 Know Your Employee Controls

The Bank of New York (BONY) correspondent banking scam highlighted how a key senior staff with the complicity of her husband helped two Russian banks to break US banking laws and move money from the US bank's accounts to third-party transferees around the world. Fraudulent loan applications were submitted supported by sham escrow agreements and executed by the bank's branch manager. Victim banks in the US lost millions of dollars. The defendants were said to have received US$1.8m in bribes from their Russian clients, allegedly linked to organized crime. US shell companies were involved in facilitating the scam.

The BONY case reveals the dangers of tapping foreign markets (like the former Soviet Union states) that are poorly regulated and high on corruption without proper compliance. It underscores the importance of know your employee controls – prescreening new employees and during the tenure of employment – especially of staff dealing with high-risk markets. The screening process must highlight accounts of other family members banking with the bank and where the employee is foreign-born it may be prudent to vet the employee’s bonafides in their home country. On an ongoing basis, the financial circumstances of employees and other situational factors should be monitored. Independent reviews and internal audits are indispensable and specifically high-risk accounts should be reviewed thoroughly including for source of funds and source of wealth.
2.7 Ongoing Transactions Monitoring

Some key red flags are that the transactions on bank accounts of shell companies frequently involve foreign payments without a clear connection to the actual activities of the corporate entity, the use of offshore bank accounts without clear economic necessity, funds transfer activity to and from high-risk jurisdictions, currency intensive transactions, and changes in the ownership or control of a private limited company followed by a significant increase in business volumes. Also watch out for new companies that have huge volumes shortly after they commence operations. Companies that are on the face of it unrelated but share the same location and/or common directorships are also a red flag.

US FinCEN Red Flags

The US FinCEN came out in August 2004 with a list of red flags for shell companies and shell banks in its 7th SAR review. They state that taken individually these indicators may not point to suspicious activities relating to shell companies or shell banks. However, used in combination with the definitions provided for shell companies, these indicators may arouse suspicions.

- An unusually high volume of wire transfer activity with multiple wire transfers totaling hundreds or thousands and with dollar amounts in the thousands or millions. These wires frequently involve originators located in high-risk regions considered vulnerable to money laundering.
- Payment originators with addresses in the country but who originate the payments from accounts held at foreign banks.
Inability to identify a location in the country, corporate officers and/or directors or the nature of the business.

Suspected shell companies based in foreign countries, which are customers of foreign banks that maintain correspondent accounts with local banks. The shell companies, through the correspondent accounts, wire funds to offshore jurisdictions.

Foreign-owned companies based in the country as originators or beneficiaries (or both) of dollar denominated wire transfers.

Numerous and large-amount wire transfers sent from offshore jurisdictions through correspondent accounts held at in-country-based banks to a foreign bank and then on to a customer’s shell corporation.

Repetitive wire transfers from a particular originator to a particular beneficiary, with one of the parties being a registered corporation in the country for which no physical location can be identified; the other party is located offshore.

Individual wire transactions conducted in large, even-dollar amounts.

Individual wire transactions conducted within a short period of time (i.e. daily basis, two times daily or every other day).

Unusually large numbers of wire transfers involving offshore correspondent account holders or domestic companies that do not appear to maintain an operating business in the state of incorporation and for which there is no indication of legitimate business activity.

In November 2006, the US FinCEN came out with a report “The Role of Domestic Shell Companies in Financial Crime and Money Laundering: Limited Liability Companies”. In the
report, the FinCEN highlighted that the following elements of suspicious activity in SARs are cited repeatedly:

- Insufficient or no information available to positively identify originators or beneficiaries of wire transfers (using internet, commercial database searches, or direct inquiries to a correspondent bank). The lack of identifying information on the transactors is one of the most frequently cited concerns.
- US company with Latvian or Russian bank account in US dollars formed in US state that does not require the reporting of information on ownership.
- Foreign correspondent bank exceeds its client profile for wire transfers in a given time period or individual company exhibits unusually high amount of activity, sometimes in bursts inconsistent with normal business patterns.
- Payments have no stated purpose, do not reference goods or services, or identify only a contract or invoice number.
- Goods or services, if identified, do not match profile of company provided by correspondent bank or character of the financial activity; companies reference remarkably dissimilar goods and services in related wire transfers (for example, computers, footwear, steel, meat products, dairy products, sporting goods, lids, auto parts, film extruders, sugar, coolers, pet resins, tissue, furs, mining machinery, maintenance and support, tutoring, marketing); explanation given by foreign correspondent bank is inconsistent with observed wire activity.
- Transacting businesses share the same address, provide only a registered agent’s address, or other address inconsistencies.
- Many or all of the wires are sent in large, round dollar, hundred dollar, or thousand dollar amounts.
- Unusually large number and variety of beneficiaries receiving wires from one company.
- Frequent involvement of high-risk offshore financial centers, especially as location of beneficiaries; sometimes many jurisdictions involved.
- Use of nested correspondent banking situations in Russia or Latvia (a high-risk foreign bank uses the correspondent account of another foreign bank).
- Repeated SAR filings on same suspects (i.e., ongoing activity over a period of months).

The SAR

The US FinCEN wants SARs on shell companies to provide the term “shell,” in the narrative and to provide all required and relevant information about the conductor(s) and transactions, including, as applicable, the names and account numbers of all originators and beneficiaries of domestic and international wire transfers, the names and locations of shell entities involved in the transfers, and the names of and information regarding any registered agents or other third parties.\(^\text{32}\)

\(^{32}\) FinCEN 7\(^{\text{th}}\) SAR Review, 2004
3. Conclusion

In conclusion, shell companies are commonly used in money laundering and now also in terrorist financing schemes. They often have a short life being setup/used for a specific transaction. Information on beneficial ownership and control is either not collected, or if collected is not properly verified in many offshore centers and there are issues with maintaining the information current and accurate over time. Whilst the FATF revised 40 principles puts pressure on countries to ensure greater standards of information collection, verification and transparency, including regulating professionals; the on-ground reality is that a number of the offshore jurisdictions have given lip-service to this due diligence issue and shell companies and trusts are created and operated just as easily as ever and continue to be exploited by criminals.